MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 212
OCTOBER 1995, PAGES 1733–1741

NEW CULLEN PRIMES

WILFRID KELLER

ABSTRACT. Numbers of the forms $C_n = n \cdot 2^n + 1$ and $W_n = n \cdot 2^n - 1$ are both called Cullen numbers. New primes C_n are presented for $n = 4713$, 5795, 6611, 18496. For W_n, several new primes are listed, the largest one having $n = 18885$. Furthermore, all efforts made to factorize numbers C_n and W_n are described, and the result, the complete factorization for all $n \le 300$, is given in a Supplement.

1. INTRODUCTION

In 1905, the Reverend J. Cullen [6] called attention to the numbers $C_n = n \cdot 2^n + 1$, the particular case of $k \cdot 2^n + 1$ where $k = n$. He observed that C_n was composite for all n in the interval $1 < n < 100$, with the only possible exception of $n = 53$. Shortly afterwards, Cunningham [7] gave the prime factor 5591 for C_{53} and restated Cullen's assertion for $1 < n \le 200$, now leaving $n = 141$ as the only uncertain case in the considered range. Cunningham pointed out that primes of the form $C_n = n \cdot 2^n + 1$ seemed to be remarkably rare.

Half a century later, in 1957, Robinson [22] showed that C_{141} was in fact a prime. Moreover, he established that this was the only prime C_n with $1 < n \le 1000$. In our numerical investigation we were able to determine four additional primes C_n. It can now be asserted that C_n is prime for $n = 1$, 141, 4713, 5795, 6611, 18496, and for no other $n \le 30000$.

The analogous numbers $W_n = n \cdot 2^n - 1$ have also been investigated. As to their primality, Riesel [21] found in 1968 that W_n is prime for $n = 2$, 3, 6, 30, 75, 81, but for no other $n \le 110$. Considerably extending this search, we could add to Riesel's list the primes W_n with $n = 115$, 123, 249, 362, 384, 462, 512, 751, 822, 5312, 7755, 9531, 12379, 15822, 18885. All other values of $n \le 20000$ yielded composite numbers.

A comprehensive study of divisibility properties of numbers C_n and W_n was presented by Cunningham and Woodall (abbreviated C & W in what follows) in 1917. On account of their classical paper [8], the notations C_n (for "Cunningham numbers") and W_n (for "Woodall numbers") have been used, while the term Cullen numbers is extended to both these varieties (cf. [13, 24]). C & W also initiated the project of actually factoring the considered numbers. This work has been extended over the past decades, inasmuch as increasingly

Received by the editor December 3, 1992 and, in revised form, March 28, 1994.
1991 *Mathematics Subject Classification*. Primary 11A51; Secondary 11B99, 11-04.
Key words and phrases. Cullen numbers, factoring, large primes.

powerful factorization methods were developed. In a Supplement to this paper the complete factorization of numbers C_n and W_n is given for all $n \le 300$.

2. Factor tables

C & W's report includes the factorization of C_n and W_n for all $n \le 32$, except for the single number W_{30}, whose primality was not recognized. In the interval $32 < n \le 66$, the character of W_n remained doubtful only for $n = 39$, 42, 51. The factor table for the original Cullen numbers C_n has subsequently been completed at least up to $n \le 43$ by Beeger [1], to $n \le 61$ by E. Karst, D. H. Lehmer and J. S. Madachy (as reported in [13]), and to $n \le 101$ by Steiner [24]. Here, three errata have to be observed: one digit is missing in each of the factorizations given for $n = 91$, 97, 101.

Also from [13] we learn that the factorizations of W_n were completed for all $n \le 49$ by Karst and Madachy, and that Madachy also factored W_n for $n = 52$, 55, 56, 57, 59, 60, and 76. The decomposition of W_{50} attributed to Lehmer gives the cofactor $1197765858343217 = 30503527 \cdot 39266471$ as a prime, and the numbers W_{123} and W_{249} are falsely reported as composites. The factors of W_{51} were later given in [24]. Finally, [13] lists small factors of numbers C_n and W_n up to $n = 300$.

In the Supplement, the complete factorization of both C_n and W_n is extended to just that limit. The tables were compiled and carefully checked by the author of this paper. Factors for $n \le 210$ considered difficult to obtain at the time were provided by G. Löh and W. Niebuhr. Thus, Löh completed C_n for $102 \le n \le 171$ and W_n to $n \le 122$ in 1984, using the methods of [2, 18, 20], and Niebuhr completed C_n and W_n for $n \le 210$ in 1986 with his implementation of the multiple polynomial quadratic sieve (MPQS) based on the description given in [23].

In 1988, H. Suyama supplied the smallest factor of W_{278} and the 16-digit prime factor of W_{211}, enabling us to prove primality for the 51-digit cofactor of this number. Suyama used his implementation of the elliptic curve method (ECM), cf. [17]. With only the exception of W_{211}, the complete range of $210 < n \le 260$ was done by the author in 1991, using the excellent factorization and prime-testing routines distributed with version 8.15 of Y. Kida's UBASIC, as released in December 1990. For a description of UBASIC, see [19]. The programs ECMX, MPQSX, and MPQSHD, written by Kida, were run on an IBM PS/2-70 386 PC equipped with a mathematical coprocessor. The most demanding application, the decomposition of the 78-digit number C_{251} into its two prime factors with MPQSHD, required 264 hours.

The completion of the final segment $260 < n \le 300$ seemed too hard for UBASIC and was therefore not attempted, leaving unfinished 16 numbers C_n and 12 numbers W_n. They were finally accomplished with the assistance of Niebuhr and R. P. Brent. Niebuhr factorized 21 of the remaining composites, using his own programs for ECM and for MPQS. The latter was run on an IBM ES/9021-440 mainframe. The largest numbers thus treated were the 77-digit cofactors of C_{261}, W_{264}, W_{267}, and W_{289}, which required about 64 hours of CPU time on the average, and the 79-digit cofactor of C_{297}, which took 81 hours.

The other seven composites had 80, 81, 83, or 86 digits. All these were attacked and finished with Brent's program MVFAC [4], a vectorized implementation of ECM. For details, see [3] and [17]. The program was run by Brent himself on a Fujitsu VP 2200/10 vector processor at the Computer Sciences Laboratory of the Australian National University, and, more intensively, on an SNI S100/10 (similar to a VP 2100/10) recently installed at the Computation Center of the University of Hamburg. Brent obtained the factorization of W_{277} (83-digit cofactor), and the author finished the remaining six numbers. The most notable factor determined with MVFAC was a 39-digit prime factor of C_{296} found after trying only 750 curves. It is also the largest "penultimate" factor contained in Tables I or II of the Supplement. The factorizations for $n \leq 300$ were completed on August 16, 1992.

Table I of the Supplement includes the factorization of $C_{128} = 2^{135} + 1$ obtained by Le Lasseur and published by Lucas [16] in 1878 (one digit in the largest factor misprinted), as well as Robinson's prime C_{141}. Table II includes the factorization of $W_{64} = 2^{70} - 1$ already contained in [16], that of $W_{128} = 2^{135} - 1$ established by P. Poulet in 1946 (see [14]), and the previously known primes. It also includes the factorizations of W_{100} and W_{256}, which, according to [13], had been completed by Karst and K. R. Isemonger, respectively. It should be noted that for $n = 100, 144, 196, 256$ the factorization of W_n was facilitated by an algebraic decomposition, as was the case historically for C_{128} and W_{128}.

C & W listed all 44 values of $n \leq 1000$ for which no factor of C_n was known and they showed that in every case the smallest factor p had to be > 1000. Precisely these C_n were tested for primality by Robinson to discover that only C_{141} was prime in that range. Apart from this prime, six more of the C_n in question, corresponding to $n = 233, 245, 251, 252, 285, 293$, are in Table I and thus completely factored. In seven cases with $n > 300$ the factorization of C_n could also be established:

$$C_{318} = 10939 \cdot 100429275849522701 \cdot \mathrm{p}78,$$
$$C_{436} = 1081501579 \cdot 43008589651 \cdot 3717967975567 \cdot \mathrm{p}102,$$
$$C_{579} = 4988803100279081295749323 \cdot \mathrm{p}153,$$
$$C_{634} = 2459 \cdot 1085629591 \cdot 2756181749 \cdot 7148901709 \cdot \mathrm{p}162,$$
$$C_{753} = 164834525239 \cdot \mathrm{p}219,$$
$$C_{921} = 2428711 \cdot 2719027 \cdot 4410839 \cdot \mathrm{p}261,$$
$$C_{933} = 197724478669 \cdot \mathrm{p}273.$$

Here pN denotes an N-digit prime. The seven cofactors, like others to be mentioned below, were proved prime by using the procedure APRT-CL (Cohen-Lenstra version of Adleman-Pomerance-Rumely Test), programmed by K. Akiyama, which is included in Kida's UBASIC. The factorization of C_{579} was obtained through MVFAC.

For 27 of the remaining 30 Cullen numbers C_n, we give in Table 1 a prime factor. If by trial division a factor p was found below 10^7, the smallest factor of C_n is tabulated. If, however, a factor $p > 10^7$ is given, it was found by one of Pollard's methods or (for $n = 581, 648, 941$) by Brent's MVFAC and might not be the least. Thus, only three Cullen numbers C_n with $n \leq 1000$ have no known factor, which are for $n = 435, 453, 915$.

TABLE 1. Prime factors p of Cullen numbers $C_n = n \cdot 2^n + 1$

n	p	n	p
333	2423	711	367957
402	1117	713	3079
412	1091	778	33667759
473	365969	816	6451
516	20641	849	7103923
532	18313	869	69508729
533	95257	870	39869
580	2843	899	1633716607
581	2660379251641	900	18176209
587	60744852593	916	247451
588	203793838081	941	77173351849725833046157080 11
609	70038149	942	2598767
648	240383530451966593	953	381287
693	134409623339		

A prime factor $p < 10^7$ does exist for all but 41 of the composite numbers W_n with $n \leq 1000$. Six of these are completely factored since they have $n \leq 300$. The following six with $n > 300$ were factored by finding one factor (in the case of W_{885}, MVFAC determined a composite factor):

$$W_{369} = 7728415141 \cdot \text{p}104,$$
$$W_{463} = 141959514756636037 \cdot \text{p}125,$$
$$W_{672} = 962794776758617477606791593 \cdot \text{p}179,$$
$$W_{789} = 738497627270005859999837 \cdot \text{p}217,$$
$$W_{885} = 8353578155864671 \cdot 84769280380290403 \cdot \text{p}237,$$
$$W_{908} = 3057961301 \cdot \text{p}267.$$

For 23 of the remaining 29, a factor $p > 10^7$ is presented in Table 2. The factor given for $n = 366$ and the smaller factor of W_{463} were kindly supplied

TABLE 2. Prime factors p of Cullen numbers $W_n = n \cdot 2^n - 1$

n	p	n	p
332	12165323	675	1608969227141
350	5169607633	722	64952161193
366	62497690394803	723	128915821
386	119570203	765	130234223449138177
423	3537292571	795	80958347
522	40818521	824	1757762099
541	3241623612714017	866	10885241
564	26768197513	906	16556069
570	48623921	931	15127751
621	16127089673	932	114082154860229
663	60166683064673819	943	405108238890652513
669	73399869877		

by H. Suyama, who found them in 1988. Those for $n = 541$, 663, 765, 932, 943 are due to MVFAC, like the above factors of W_{672} and W_{789}. The numbers W_n without a known factor now occur for $n = 349$, 375, 668, 715, 951, 963.

There is presently a project underway attempting complete factorizations for the whole range $300 < n \leq 1000$. As of the end of February 1994, 147 numbers C_n and 142 numbers W_n had virtually been finished. A machine readable list with all known factors is available from the author, who would welcome any new factors that readers may wish to contribute.

3. Divisibility properties

In pursuance of the original observations made by Cullen and by Cunningham, a glance at the factor table for C_n suggests that a prime p divides both the numbers C_{p-1} and C_{p-2}. A more general statement is in fact true. For a given odd prime p let $n_k = (2^k - k)(p-1) - k$, $k \geq 0$. This includes $n_0 = p-1$ and $n_1 = p-2$. The statement is that p divides C_{n_k} for all $k \geq 0$, and it is verified easily. Since $n_k \equiv -2^k \pmod{p}$, we have $n_k \cdot 2^{n_k} \equiv -2^{k+n_k} \equiv -2^{(2^k-k)(p-1)} \pmod{p}$, which by Fermat's theorem is congruent to -1 modulo p. Therefore $C_{n_k} \equiv 0 \pmod{p}$. Obviously, n_k cannot be a multiple of p.

To describe the totality of numbers C_n that are divisible by a given prime p, two remarks are in order. First, the numbers $C_n \bmod p$ are periodic with period ph_p, where $h_p = \exp_p(2)$ is the smallest positive integer h such that $2^h \equiv 1 \pmod{p}$. As a consequence, if p divides C_n for some n, then p also divides C_{n+ph_p}. Secondly, from the definition of n_k it may be deduced that there are exactly h_p numbers n_k which are incongruent modulo ph_p, and no other n with $0 < n < ph_p$ gives a C_n with a prime factor p (cf. [8]). So, the totality of all n such that C_n is divisible by p is obtained as follows. Determine $n'_k = n_k \bmod ph_p$ for $k = 0, 1, \ldots, h_p - 1$, $0 < n'_k < ph_p$. Then, for every k, include $n = n'_k + rph_p$ for all $r \geq 0$.

In particular, the prime $p = 3$ divides all C_n with $n \equiv 1, 2 \pmod{6}$. As a further example, for $p = 11$, $h_p = 10$, we get $n'_k = 10$, 9, 18, 47, 6, 45, 24, 103, 52, 71, and all integers n congruent modulo 110 to any one of these.

A similar description can be given for the set of subscripts n for which W_n is divisible by p. Let $n_k = -(2^k + k)(p-1) - k$ (these are negative integers) for $k \geq 0$, determine $n'_k = n_k \bmod ph_p$ for $k = 0, 1, \ldots, h_p - 1$, $0 < n'_k < ph_p$, and, for every k, include $n = n'_k + rph_p$ for all $r \geq 0$. In this case, $p = 3$ divides all W_n with $n \equiv 4, 5 \pmod{6}$, and $p = 11$, $h_p = 10$ give $n'_k = 100$, 79, 48, 107, 16, 65, 64, 73, 102, 61, and all n congruent modulo 110 to any one of these.

Note that for $n = 65$, 64 we have two consecutive numbers W_n, and actually an infinity of such pairs, which are both divisible by the same prime $p = 11$. For numbers C_n this situation occurs for every prime p, as we have seen. For numbers W_n, however, this is restricted to the case that h_p is an even number. The minimality of h_p then implies that $2^{h_p/2} \equiv -1 \pmod{p}$ and thus also $2^{ph_p/2} \equiv -1 \pmod{p}$. It is now easily seen that $W_n \equiv 0 \pmod{p}$ for $n = ph_p/2 + p - 1$ and for $n = ph_p/2 + p - 2$.

Other divisibility rules are also contained in the given general description.

For instance, p divides $C_{(p+1)/2}$ and $W_{(3p-1)/2}$, or it divides $C_{(3p-1)/2}$ and $W_{(p+1)/2}$, according as the Jacobi symbol $(2/p)$ is -1 or $+1$. Again, this can be verified immediately. For more details, see [7] and [8].

In spite of the apparent similarity in the description of small factors for both sequences $\{C_n\}$ and $\{W_n\}$, considerably more composites are obtained for the original Cullen numbers C_n. This is primarily due to the fact that every prime $p > 3$ immediately gives four consecutive composite numbers C_n. In addition to C_{p-1} and C_{p-2}, always two neighboring numbers of the sequence are divisible by 3. If p is of the form $p = 6k + 1$, then 3 divides C_p and C_{p+1}, and in the case of $p = 6k - 1$, the prime 3 divides C_{p-3} and C_{p-4}. In the special situation of a twin prime pair $p, q = 6k \pm 1$, together a string of eight consecutive composites C_n occurs.

To give an indication of how the notable difference in the number of primes of the forms C_n and W_n comes about, let us first consider all values of $n \leq 110$ such that C_n has no prime factor $p \leq n + 2$. Here we get $n = 33, 53, 75$, where $n = 75$ can be eliminated through the prime factor $p = 2n - 1 = 149$. In the case of W_n, however, 32 values of n remain in the first step, of which eight are eliminated by a factor $p = 2n - 1$. The remainder of 24 includes, of course, the six values of $n \leq 110$ giving rise to the primes W_n determined by Riesel.

4. Cullen primes

In our search for new primes, we tested C_n for $n \leq 20000$ in 1984 and continued (without success) to $n \leq 30000$ in 1987. Similarly, W_n was tested up to $n \leq 15000$ in 1984, and to $n \leq 20000$ in 1987. In this case two more primes were found for $n = 15822$ and $n = 18885$. All other new Cullen primes were thus discovered in 1984. The methods used for proving primality are found in [5]. For $1000 < n \leq 20000$, a total of 632 numbers C_n and 1203 numbers W_n had actually to be tested after the sieving procedure. In addition, 321 numbers C_n with $20000 < n \leq 30000$ remained without known factor. We also considered the possibility of $n \cdot 2^n \pm 1$ forming a pair of twin primes. Such "Cullen twins" may indeed exist for some large n. But we showed (by testing individual numbers C_n) that this n must exceed $n = 41528$.

The prime $C_{18496} = 17^2 \cdot 2^{18502} + 1 = (17 \cdot 2^{9251})^2 + 1$ might be of some interest in relation to Conjecture E of Hardy and Littlewood [10], which states that an infinity of primes $N^2 + 1$ should exist (actually, the conjecture was given in a quantitative asymptotic form). At the time of its discovery, our prime seemed to be the largest one known of that expression. But now we know five larger ones, discovered by H. Dubner (unpublished), which are of the form $b^{2^m} + 1$, with b even. The largest of these primes is $200944^{2^{11}} + 1$, which has 10861 digits and was found in September, 1992. Incidentally, Dubner [9] has also considered a generalization of Cullen numbers given by $n \cdot b^n + 1$ for $b > 2$.

Regarding the primes W_n listed for $n > 110$, it appeared that four of them had already been known for some time. As a matter of fact, Williams and Zarnke [25] had found W_{115} to be prime, Jönsson [12] had found $181 \cdot 2^{363} - 1 = W_{362}$, Riesel [21] had given $3 \cdot 2^{391} - 1 = W_{384}$, and W_{512} turned out to be the Mersenne prime $M_{521} = 2^{521} - 1$ discovered by Robinson (see [15]).

A first result concerning the distribution at large of Cullen primes C_n was obtained by Hooley [11]. By applying sieve methods, he showed that the natural density of positive integers $n \leq x$ for which C_n is a prime is of the order $o(x)$ for $x \to \infty$. In that sense, almost all Cullen numbers are composite. Suyama (communicated personally) has reworked Hooleys proof to show that it is applicable to any sequence of numbers $n \cdot 2^{n+a} + b$, where a, b are arbitrarily fixed integers. In particular, Hooley's result also follows for numbers W_n.

In the context of a search for prime factors of Fermat numbers our particular interest in Cullen numbers C_n emanated from the remark of C & W, supported by an explicit argument, that primes of the form C_n seemed likely as possible divisors of Fermat numbers. However, the four new primes C_n proved not to divide any of these.

Instead, there is some evidence for the likelihood that a prime W_n divides a Mersenne number M_p. We noticed that $W_2 = M_3$ and $W_{512} = M_{521}$, and that W_3 divides M_{11}, W_6 divides M_{191}, and W_{123} divides M_p for $p = 123 \cdot 2^{122} - 1$, a 39-digit prime. In all three cases where W_n properly divides M_p, we have $p = (W_n - 1)/2 = n \cdot 2^{n-1} - 1$, that is, p and the divisor $W_n = 2p+1$ are both primes.

To establish in general whether W_n divides any M_p or not, the complete factorization of $(W_n - 1)/2$, if available, can be used. In fact, a divisor W_n of M_p must also be of the form $2kp + 1$. Equivalently, $(W_n - 1)/2 = kp$, hence the particular subscript p should divide $(W_n - 1)/2$. So, for all different prime factors p of this number, one would have to check if $M_p \bmod W_n = 0$. But in practice a much easier test suffices, as Suyama has indicated in a personal communication. To see whether a prime q divides some Mersenne number or not, only an "evenly factored portion" of $q - 1$ and its cofactor need to be used.

Let q be a prime and $q - 1 = 2^{\alpha_0} \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_r^{\alpha_r} \cdot C$, where p_j are odd primes and C is composite. If $2^{p_j} \not\equiv 1 \pmod{q}$ for $1 \leq j \leq r$ and $2^C \not\equiv 1 \pmod{q}$, then q cannot be a factor of any Mersenne number. In the alternative case that $2^C \equiv 1 \pmod{q}$, q may be a factor of M_p, where p is some prime factor of C. Indeed, if for an unknown factor p of C we had $q \mid M_p$, that is $2^p \equiv 1 \pmod{q}$, then necessarily $2^C \equiv 1 \pmod{q}$.

For all primes $q = W_n$ with $30 \leq n \leq 822$ (except for the otherwise settled $n = 123$) this test was conclusive by using only one odd factor p_1 of $W_n - 1$. In most cases, a very small p_1 was readily found, while for $n = 249$ and $n = 384$ the factors $p_1 = 708211533214392631$ resp. $p_1 = 12694590781$ determined by Suyama had to be used. It has also been checked that the Cullen number W_{5312} does not divide any Mersenne number, by calculating $2^C \bmod W_{5312}$ for $C = (W_{5312} - 1)/(2 \cdot 3 \cdot 5^2)$. But here we had the interesting case that, nevertheless, $2^{C'} \equiv 1 \pmod{W_{5312}}$ for $C' = (W_{5312} - 1)/(2 \cdot 3)$. For W_{7755}, the test could not be carried out, because no factor of the composite number $(W_{7755} - 1)/2$ was found. Recently, Dubner has kindly tested the numbers W_n for $n = 9531$, 12379, 15822, 18885, without detecting a divisibility. In the case of $n = 15822$ he obtained $2^C \equiv 1 \pmod{W_{15822}}$, where $C = (W_{15822} - 1)/(2 \cdot 7)$ and no further factor of this number was known.

Of course, W_n may also be identical to a Mersenne number without being a prime. Generally, W_n is a Mersenne number whenever $n = 2^m$ and $m + 2^m$ is prime. This is the case for $m = 1$: $W_2 = M_3 = 7$; $m = 3$: $W_8 = M_{11} = 23 \cdot 89$; $m = 5$: $W_{32} = M_{37} = 223 \cdot 616318177$; $m = 9$: $W_{512} = M_{521}$; and also for $m = 15$, 39, 75, 81, 89, 317, 701, 735 and no other $m \leq 1310$.

5. Biographical note

When we searched the literature for references to Cullen numbers, we were intrigued by the fact that almost nothing could be found about Cullen as a person. Even mathematical or encyclopaedic dictionaries usually giving such information failed to disclose Cullen's complete first name or to mention the year of his birth or his death. Only the abbreviation "S. J." placed after his name in a footnote to [8] suggested that he was a Jesuit priest. That hint finally enabled us to locate the most appropriate and authoritative source for this matter, namely, the Department of Historiography and Archives of the English Province of the Society of Jesus. The archivist of that institution, Father T. G. Holt, was kind enough to provide the following biographical data, which we are pleased to present to the reader in unabridged form.

> Father James Cullen, S. J., was born on April 19th 1867 at Drogheda in Ireland. At first he was educated privately, then by the Christian Brothers. Next he went to Trinity College, Dublin, to study pure and applied Mathematics. Afterwards he was in business for a while, but after a short period at an apostolic school in Ireland to learn Latin he entered the noviceship of the English Jesuits at Manresa House, Roehampton, London, as he had decided to become a priest. From 1892 till 1895 he was at Manresa in the noviceship and then for a year's study. From 1895 till 1897 he studied philosophy at the Jesuit house for philosophical studies at St Mary's Hall, Stonyhurst in Lancashire. From 1897 till 1901 he studied theology at the theologate of the English Jesuits at St Beuno's College in North Wales. He was ordained priest at St Beuno's College on July 31st 1901. In 1902 and 1903 he taught Mathematics to young Jesuits who had finished their noviceship at Manresa House. In 1905 he taught Mathematics at the Jesuit boarding school Mount St Mary's College in Derbyshire. It is said that he found difficulty in teaching. In 1906 he was sent to Stonyhurst College, also a boarding school, as accountant and later manager of the College farm and estate. Meanwhile he kept in touch with leading mathematicians and contributed articles to *Nature*, the *Mathematical Gazette* and the *Messenger of Mathematics*. In 1921 he left Stonyhurst and was appointed to supervise accounts of other English Jesuit houses. He died on December 7th 1933.

Acknowledgments

The author thanks Hiromi Suyama for his remarks and suggestions indicated in the text, as well as for the provision of some prime factors, and to Günter Löh for the factorizations mentioned in §2. Thanks are also due to Wolfgang Niebuhr for his willingness to produce difficult factorizations whenever asked to do so. He has been appropriately included as a coauthor of the Supplement in acknowledgment of the substantial contributions he has made to it over the years. Special thanks are extended to Richard Brent for making available his program MVFAC and thus allowing us to obtain the last factorizations needed to complete the Supplement.

Finally, the author is greatly indebted to Father Bruno Brinkman of Heythrop College, University of London, for helping to establish contact with Father Geoffrey Holt, who compiled and wrote the enlightening biographical note of §5.

BIBLIOGRAPHY

1. N. G. W. H. Beeger, *Cullen numbers*, MTAC **8** (1954), 188.
2. R. P. Brent, *An improved Monte Carlo factorization algorithm*, BIT **20** (1980), 176–184.
3. ——, *Some integer factorization algorithms using elliptic curves*, Austral. Comput. Sci. Comm. **8** (1986), 149–163.
4. ——, *MVFAC: A vectorized Fortran implementation of the elliptic curve method*, Comput. Sci. Lab., Austral. Nat. Univ., 1991.
5. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, 2nd ed., Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1988.
6. J. Cullen, *Question 15897*, Educ. Times, Dec. 1905, 534.
7. A. Cunningham, *Solution of Question 15897*, Math. Quest. Educ. Times **10** (1906), 44–47.
8. A. Cunningham and H. J. Woodall, *Factorisation of* $Q = (2^q \mp q)$ *and* $(q.2^q \mp 1)$, Messenger Math. **47** (1917), 1–38.
9. H. Dubner, *Generalized Cullen numbers*, J. Recreational Math. **21** (1989), 190–194.
10. G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio numerorum'*; III: *On the expression of a number as sum of primes*, Acta Math. **44** (1923), 1–70.
11. C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge Univ. Press, Cambridge, 1976.
12. I. Jönsson, *On certain primes of Mersenne-type*, BIT **12** (1972), 117–118.
13. E. Karst, *Prime factors of Cullen numbers* $n \star 2^n \pm 1$, Number Theory Tables, compiled by A. Brousseau, Fibonacci Assoc., San Jose, Calif., 1973, pp. 153–163.
14. D. H. Lehmer, *On the factors of* $2^n \pm 1$, Bull. Amer. Math. Soc. **53** (1947), 164–167.
15. ——, *Recent discoveries of large primes*, MTAC **6** (1952), 61.
16. E. Lucas, *Sur la série récurrente de Fermat*, Bull. Bibl. Storia Sc. Mat. Fis. **11** (1878), 783–798.
17. P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), 243–264.
18. M. A. Morrison and J. Brillhart, *A method of factoring and the factorization of* F_7, Math. Comp. **29** (1975), 183–205.
19. W. D. Neumann, *UBASIC: a Public-Domain BASIC for Mathematics*, Notices Amer. Math. Soc. **36** (1989), 557–559; *UBASIC Update*, ibid. **38** (1991), 196–197.
20. J. M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528.
21. H. Riesel, *Lucasian criteria for the primality of* $N = h \cdot 2^n - 1$, Math. Comp. **23** (1969), 869–875.
22. R. M. Robinson, *A report on primes of the form* $k \cdot 2^n + 1$ *and on factors of Fermat numbers*, Proc. Amer. Math. Soc. **9** (1958), 673–681.
23. R. D. Silverman, *The multiple polynomial quadratic sieve*, Math. Comp. **48** (1987), 329–339.
24. R. P. Steiner, *On Cullen numbers*, BIT **19** (1979), 276–277.
25. H. C. Williams and C. R. Zarnke, *A report on prime numbers of the forms* $M = (6a+1)2^{2m-1} - 1$ *and* $M' = (6a-1)2^{2m} - 1$, Math. Comp. **22** (1968), 420–422.

REGIONALES RECHENZENTRUM DER UNIVERSITÄT HAMBURG, 20146 HAMBURG, FEDERAL REPUBLIC OF GERMANY

E-mail address: keller@rrz.uni-hamburg.de